🧾 Phishing Simulation Report

Prepared by: Joshwa
Internship at: Future Intern
Date: 27/05/2025
Tool Used: SET (Social Engineering Toolkit)

📌 1. Executive Summary

This report documents a phishing simulation using the Social Engineering Toolkit (SET), hosted locally to test awareness and behavior toward phishing techniques. The objective was to understand how cloned login pages can be used to harvest credentials and how users react to them, within a safe, educational context.

🎯 2. Objective

- Demonstrate a phishing attack using a cloned web page.
- Host the phishing page locally and observe credential capture.
- Highlight the need for awareness, even in controlled environments.

🛠️ 3. Tool Used

Tool: Social Engineering Toolkit (SET)
Modules Used:

- Website Attack Vectors → Credential Harvester
- Site Cloned: Instagram login page

Attack Type:

- Credential Harvesting via Cloned Website

🧪 4. Simulation Details

Parameter	Description
Simulation Name	Local Phishing Test
Phishing Method	Credential Harvester
Target	A trusted friend (for testing purposes)
Clone Source	Instagram login page
Hosting Method	Apache server (localhost)
Simulation Duration	1 hour

📊 5. Results Summary

Metric	Value
User Visited the Link	5
Credentials Captured	2
Page Load Success	✅
Apache Log Recorded	✅

📝 Captured credentials were visible in the `harvester` log and were for **demo/testing** only.

🔍 6. Observations

- The cloned page appeared visually similar to the real site.
- The friend entered credentials without verifying the URL.
- Credentials were successfully logged on the backend.
- SET's toolset proved effective for ethical simulation purposes.

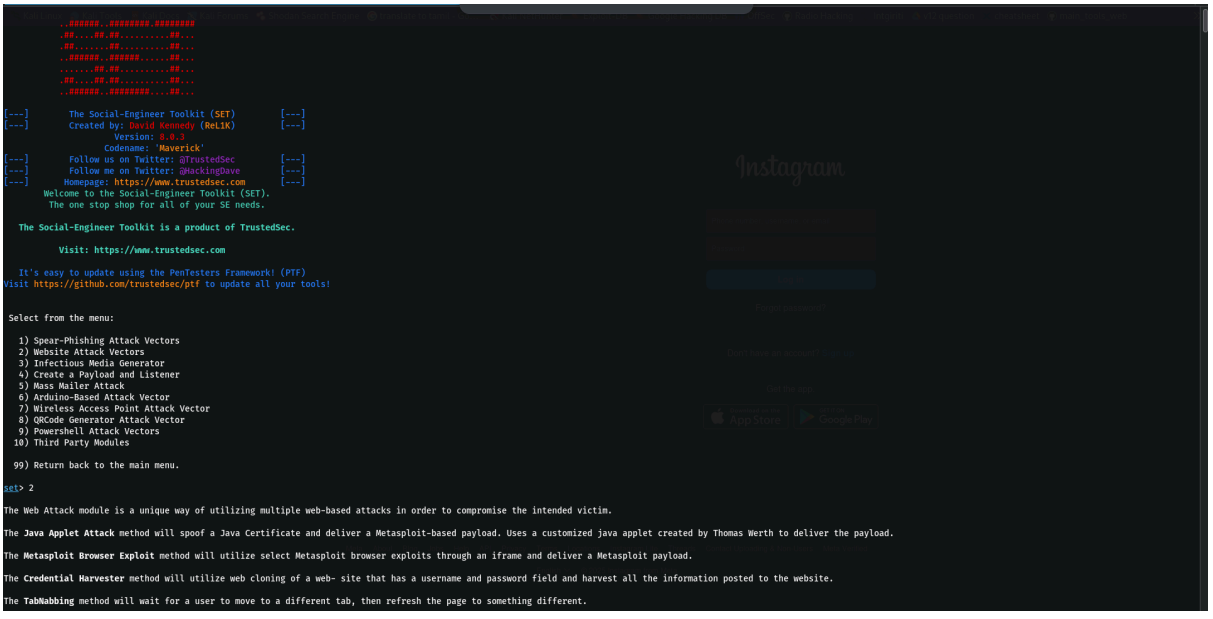
💡 7. Learning Outcome

- Users may unknowingly trust a phishing page if it mimics a real one closely.
- Visual similarity and lack of awareness are common causes of phishing success.
- Even tech-aware individuals may overlook key red flags like the URL bar.

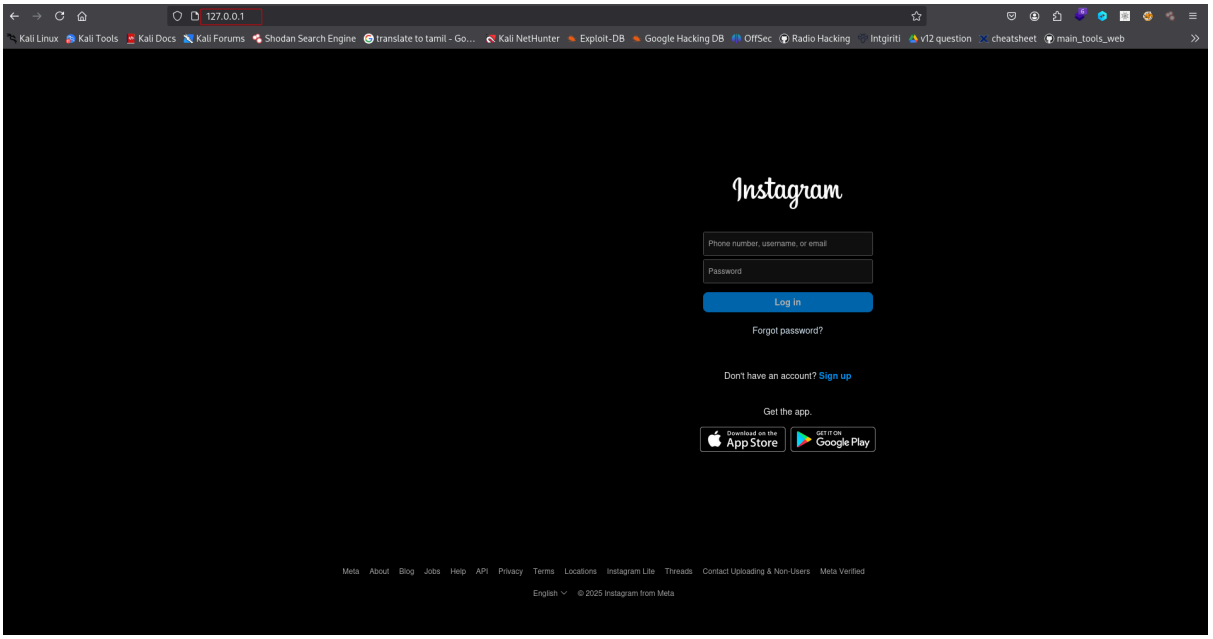
📚 8. Recommendations

- Always verify URLs before entering login information.
- Raise awareness on phishing techniques through short training.
- Use tools like password managers to detect URL mismatch.
- Promote the habit of reporting suspicious web pages or links.

📎 9. Screen Shots



```
The HTA Attack method will allow you to clone a site and perform PowerShell injection through HTA files which can be used for Windows-based PowerShell exploitation through the browser.

   1) Java Applet Attack Method
   2) Metasploit Browser Exploit Method
   3) Credential Harvester Attack Method
   4) Tabnabbing Attack Method
   5) Web Jacking Attack Method
   6) Multi-Attack Web Method
   7) HTA Attack Method

  99) Return to Main Menu

set:webattack>3

 The first method will allow SET to import a list of pre-defined web
 applications that it can utilize within the attack.

 The second method will completely clone a website of your choosing
 and allow you to utilize the attack vectors within the completely
 same web application you were attempting to clone.

 The third method allows you to import your own website, note that you
 should only have an index.html when using the import website
 functionality.

   1) Web Templates
   2) Site Cloner
   3) Custom Import

  99) Return to Webattack Menu

set:webattack>2
[-] Credential harvester will allow you to utilize the clone capabilities within SET
[-] to harvest credentials or parameters from a website as well as place them into a report

--------------------------------------------------------------------------------
--- * IMPORTANT * READ THIS BEFORE ENTERING IN THE IP ADDRESS * IMPORTANT * ---

The way that this works is by cloning a site and looking for form fields to
rewrite. If the POST fields are not usual methods for posting forms this
could fail. If it does, you can always save the HTML, rewrite the forms to
be standard forms and use the "IMPORT" feature. Additionally, really
important:

If you are using an EXTERNAL IP ADDRESS, you need to place the EXTERNAL
IP address below, not your NAT address. Additionally, if you don't know
basic networking concepts, and you have a private IP address, you will
need to do port forwarding to your NAT IP address from your external IP
address. A browser doesn't know how to communicate with a private IP
address, so if you don't specify an external IP address if you are using
this from an external perspective, it will not work. This isn't a SET issue
this is how networking works.
```




```
POSSIBLE USERNAME FIELD FOUND: route_urls[1]=/accounts/emailsignup/
PARAM: routing_namespace=igx_www$a$87a091182d5bd65bcb043a2888004e09
PARAM: __d=www
POSSIBLE USERNAME FIELD FOUND: __user=0
PARAM: __a=1
PARAM: __req=h
PARAM: __hs=20236.HYP:instagram_web_pkg.2.1...0
PARAM: dpr=2
PARAM: __ccg=GOOD
PARAM: __rev=1023248000
PARAM: __s=czsage:56af8r:sxr2pe
PARAM: __hsi=7509501377768601159
PARAM: __dyn=7xeUjG1mxu1syUbFp41twpUnwgU29zEdEc8co2qwJw5ux609vCwjE1EE2Cw8G1Dz81s8hwGxu786a3a1YwBgao6C0Mo2swaOfK0EUjwGzEaE2iwNwmE2eUlwhE2Lw6OyES1TwVwDwHg2ZwrUdUbGweG269wr86C1mgcEed6goK10xKi2qi7E5y1rwcObBKu9w4UwFw
PARAM: __csr=gnf35ndsWQyiTlFHqOQWrKFGAWAmiGAXh98yGAhKbiNDmnXhVFFqyovz8g-Uiy44FHG9Dwwgjjh4te8gmhWxnJu7bGWAAG7EcUXzt5LUsxprz8Cqq8x66omBDwYxaFE-BzEgXwho01iFy0BKE37w50a0mwi1YycYUkwzwKw6ewc5w9e0JE5e0qqO29y0coo2mg6G5pm581kcUfU11jw5rJk7Uao1hpng0rzCw9900pP80XW0ui
PARAM: __comet_req=7
PARAM: lsd=AVrzyJ2oBJI
PARAM: jazoest=2946
POSSIBLE PASSWORD FIELD FOUND: __spin_r=1023248000
POSSIBLE PASSWORD FIELD FOUND: __spin_b=trunk
POSSIBLE PASSWORD FIELD FOUND: __spin_t=1748442039
PARAM: __crn=comet.igweb.PolarisHomeRoute
[*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.


[*] WE GOT A HIT! Printing the output:
POSSIBLE PASSWORD FIELD FOUND: enc_password=#PWD_INSTAGRAM_BROWSER:10:1748442108:AeBQAEW57i25Gw4vvLI1jfm0yK+w6jCE2G5lUk56M7eYj1JXNANvC/dTlU3mrb5kEirIoMpFmi6dxPMlyMSyhyoPBD80ClgcFjdG/uDcaKJdah5tci47wyq6grUqCsBdPcCtkDurxuOtuw==
PARAM: caaF2DebugGroup=0
PARAM: isPrivacyPortalReq=false
POSSIBLE USERNAME FIELD FOUND: loginAttemptSubmissionCount=0
PARAM: optIntoOneTap=false
PARAM: queryParams={}
PARAM: trustedDeviceRecords={}
POSSIBLE USERNAME FIELD FOUND: username=hi
PARAM: jazoest=21931
[*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.
```

Password

Username

✅ 10. Conclusion

This phishing simulation demonstrates the effectiveness of cloned websites in capturing user credentials. Even in small-scale tests, phishing remains a powerful social engineering tactic. Awareness and vigilance are essential.
